

FIG 1

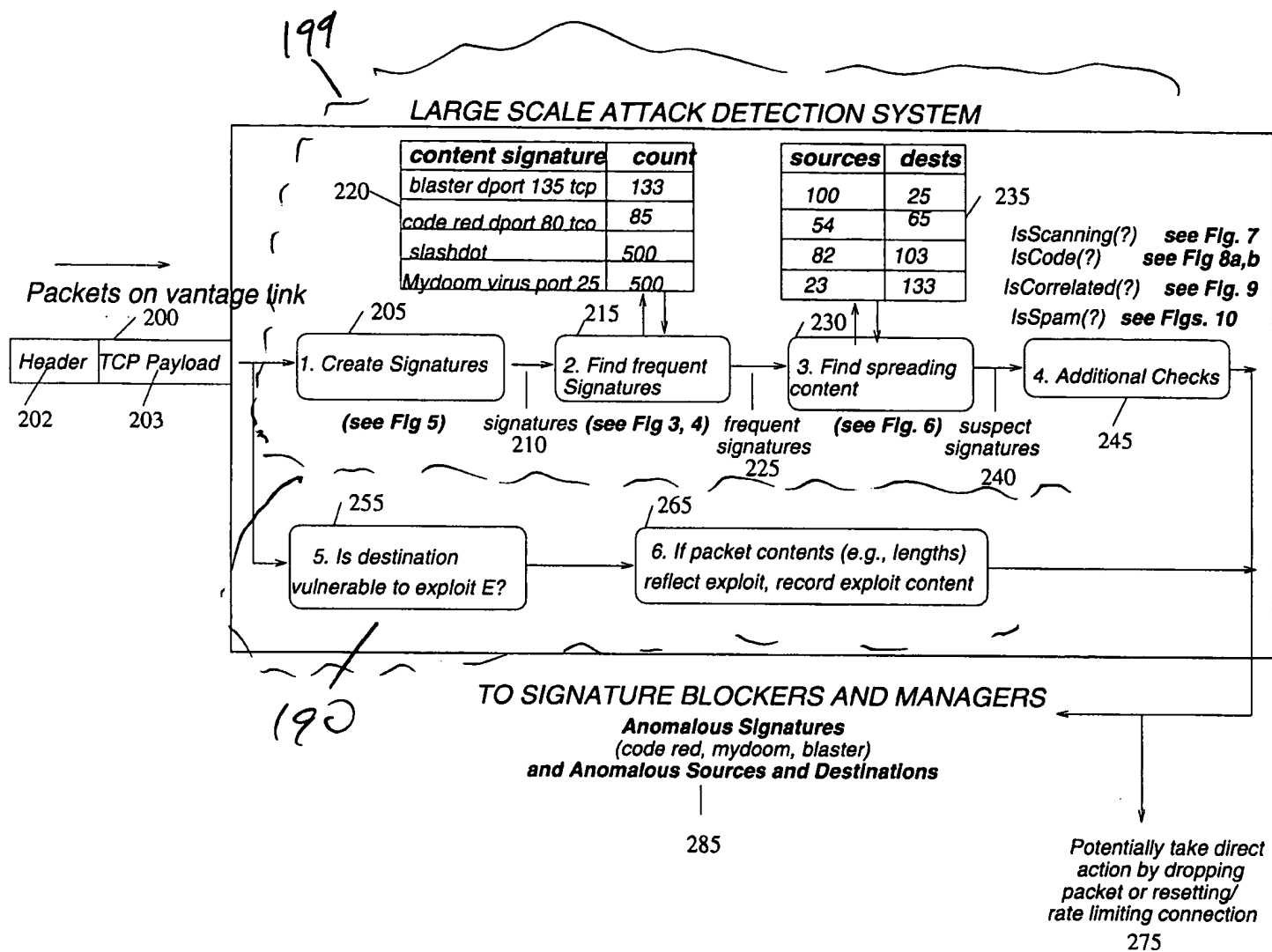


Figure 2: Large Scale Intrusion Detection System

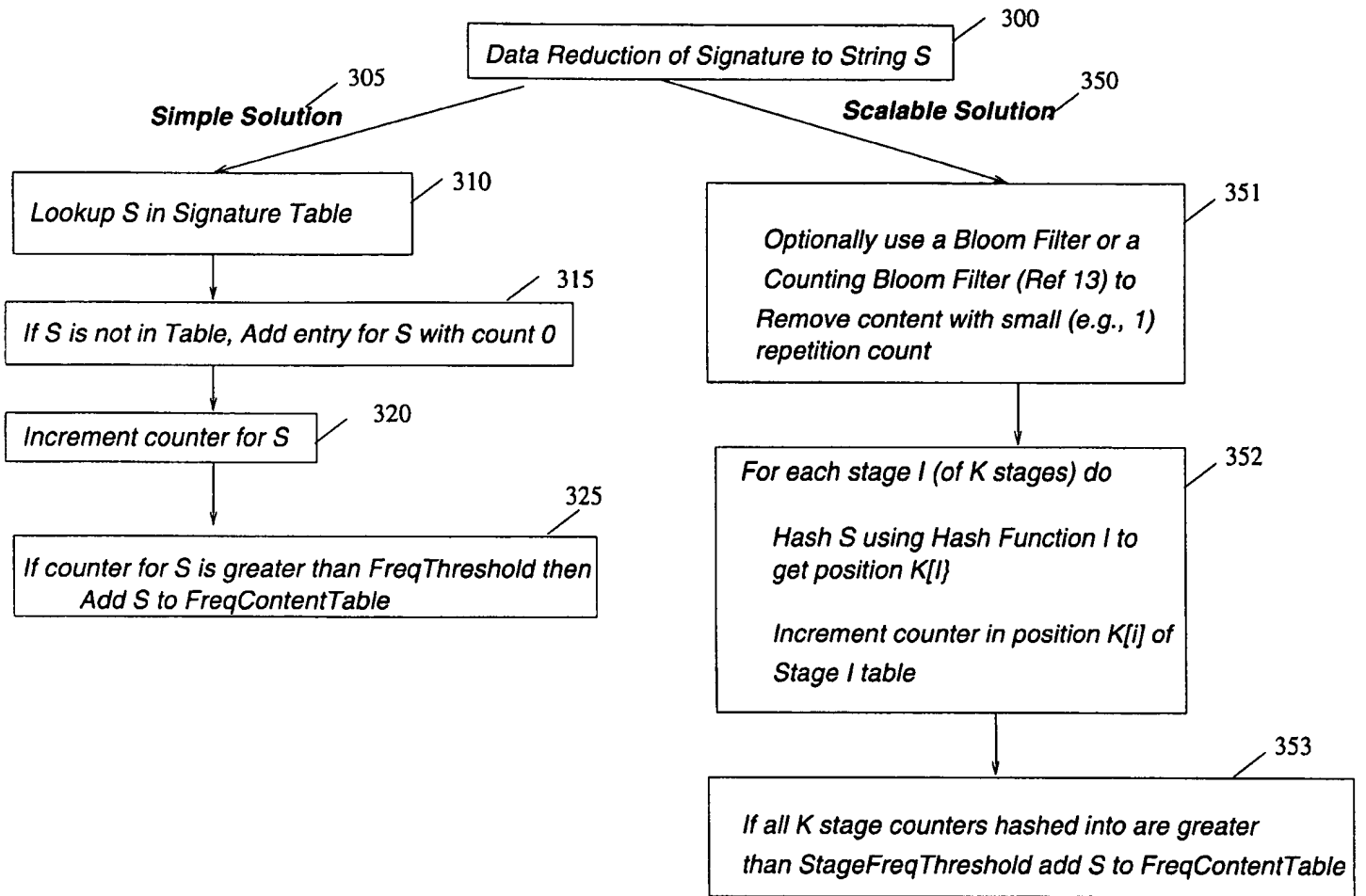


Figure 3: This figure shows the details of Block 215 of the LSIDS system of Figure 2. It sieves out frequent signatures for entry into the $FrequentContentTable$. Two alternatives are described, a simple version and a scalable version.

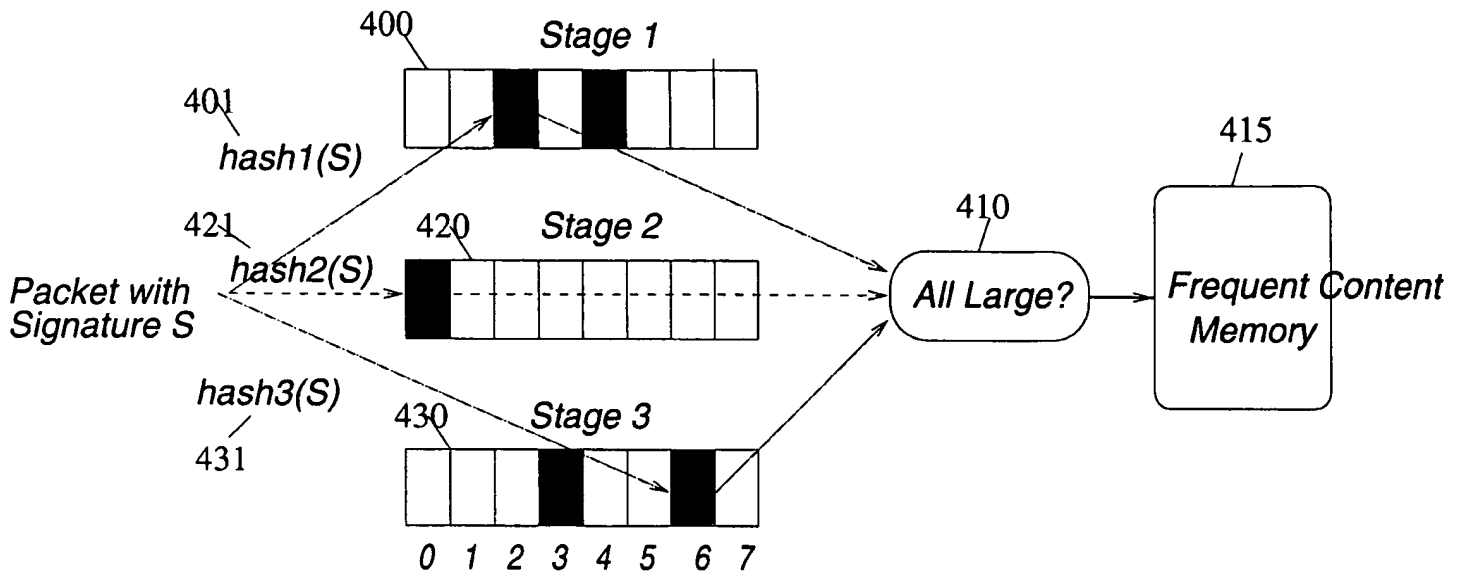


Figure 4: To identify frequent content using only a small amount of memory, a packet with content C is hashed using hash function $hash1$ into a Stage 1 hash table, $hash2$ into a Stage 2 hash table, etc. Each of the hash buckets contain a counter that is incremented by 1. If *all* the hash bucket counters are above the threshold (shown black), then content C is passed to the frequent content table for more careful observation.

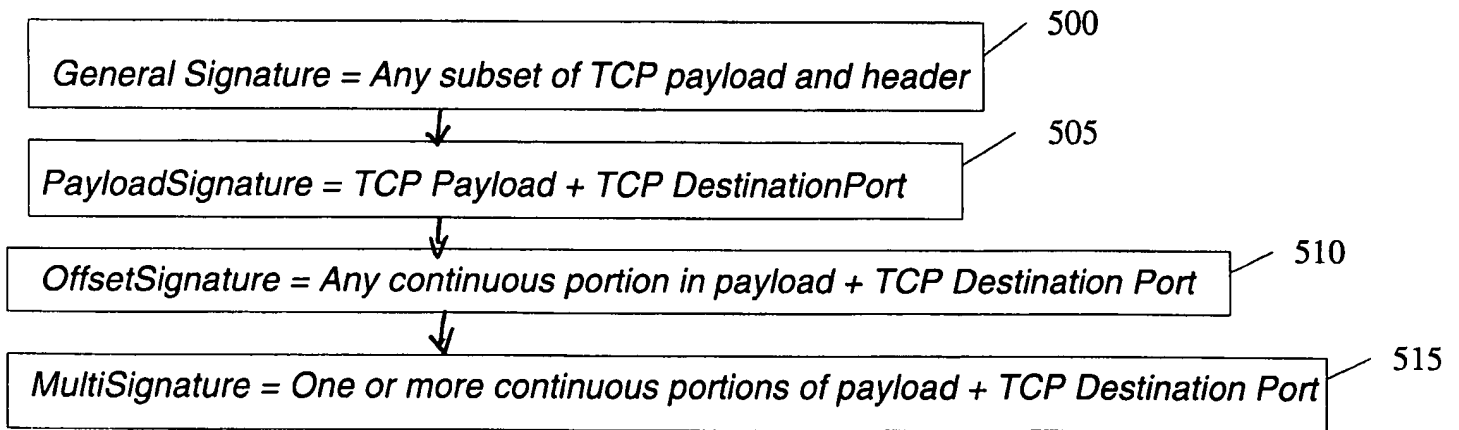


Figure 5: This figure shows the details of Block 205 of the USIDS system of Figure 2.

When string *S* is added to FreqContentTable

Figure 6a

Initialize SourceBitMap and DstBitMap to zeroes and SourceScale to SThreshBits and DestScale to DThreshBits

When processing a packet with hashed signature *S*

Lookup entry for *S* in FreqContentTable, skip remaining steps if not found

650

Hash Source IP Address of Packet to a *W* bit number *Shash*
 Let *r* be the number of bits in SourceBitMap corresponding to *S*

655

If all bits in *Shash* from positions *r*+1 through *r* + SourceScale are all 0 then
 Set position *x* in SourceBitMap to 1 where *x* is low order *r* bits of *Shash*

660

Hash Destination IP Address of Packet to a *W* bit number *Dhash*
 Let *t* be the number of bits in DestBitMap corresponding to *S*

665

If all bits in *Dhash* from positions *t*+1 through *t* + DestScale are all 0 then
 Set position *y* in DestBitMap to 1 where *y* is low order *r* bits of *Dhash*

670

If bits set in SourceBitMap * $2^{\text{SourceScale} - 1} > \text{SourcesThreshold}$ and
 bits set in DestBitMap * $2^{\text{DestScale} - 1} > \text{DestThreshold}$ then
 Add signature *S* to suspicious table if not there already
 Log SourceCount and DestCount to entry in Suspicion Table
 Initialize SourceBitMap and DestBitMap for *S* to zeroes
 Increment SourceScale and DestScale to allow counting twice as much next time

Figure 6c

Figure 6: This figure shows the details of block 230 of the USIDS system of Figure 2. It shows how frequent signatures are checked for signs of large scale involvement and rising infection levels. Such signatures are entered in the suspicious signature table and their source count and destination counts are logged to record the progress of the infection.

scale up
 by scale factor

Form 1 bit
counting array

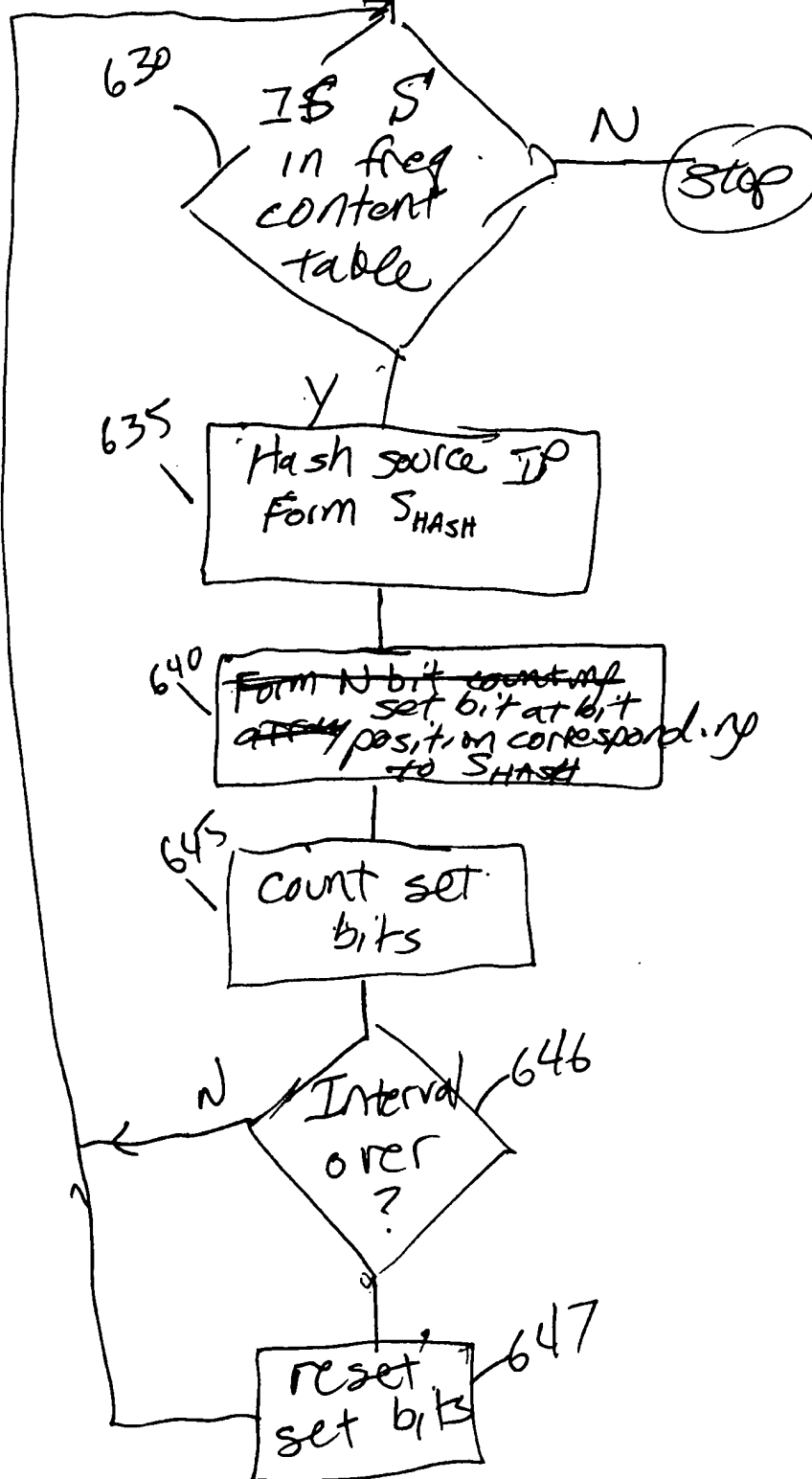
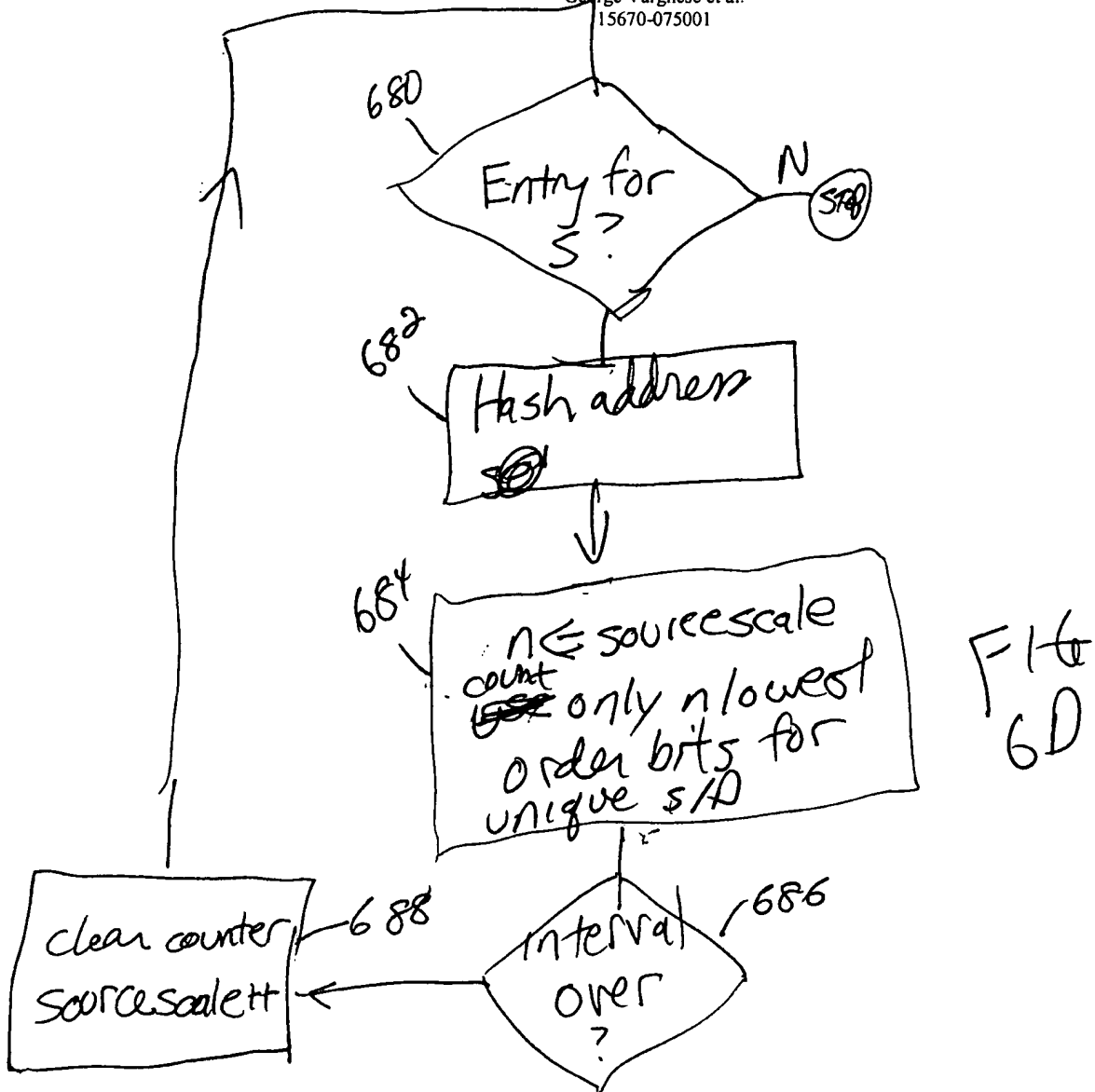


FIG
6B



Test for Content that Scans

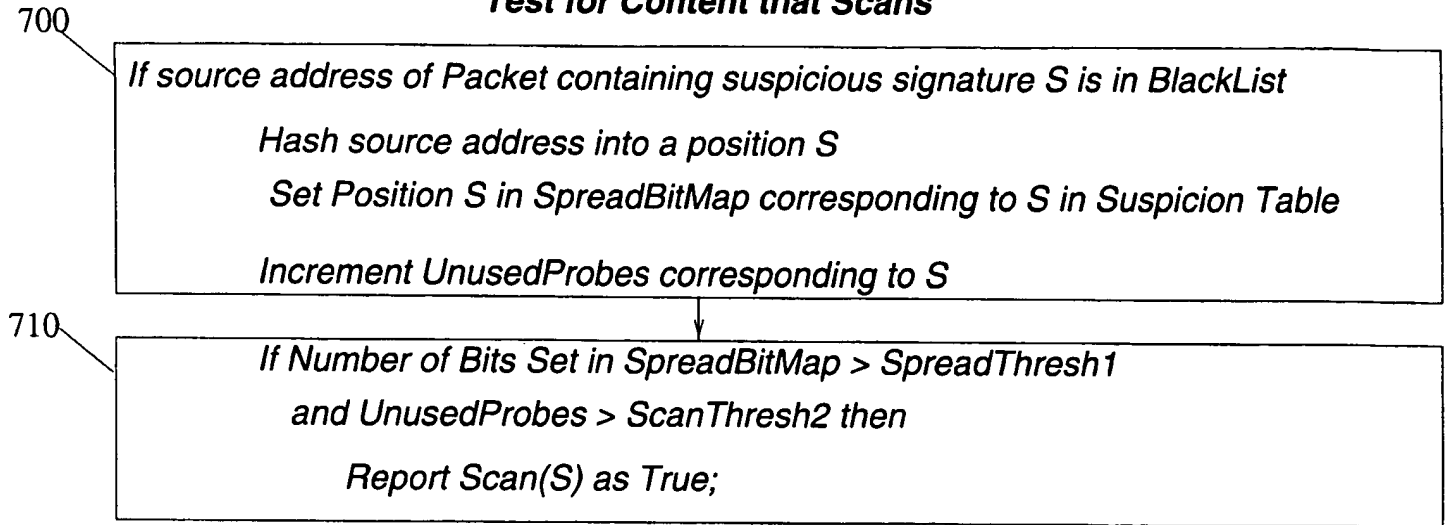
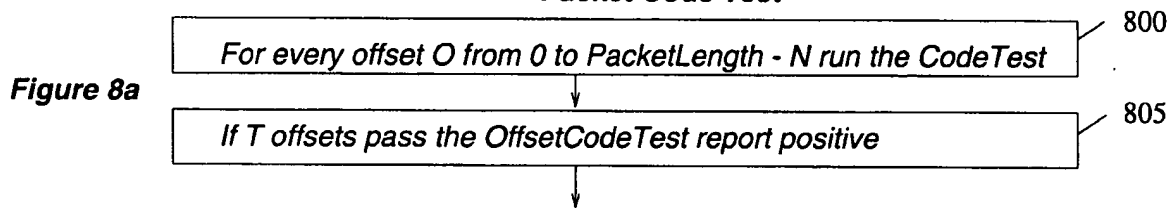


Figure 7: Soan test as part of the further tests (245) of the LSIDS system of Figure 2

Packet Code Test



OffsetCodeTest at Offset *O* for Length *N*

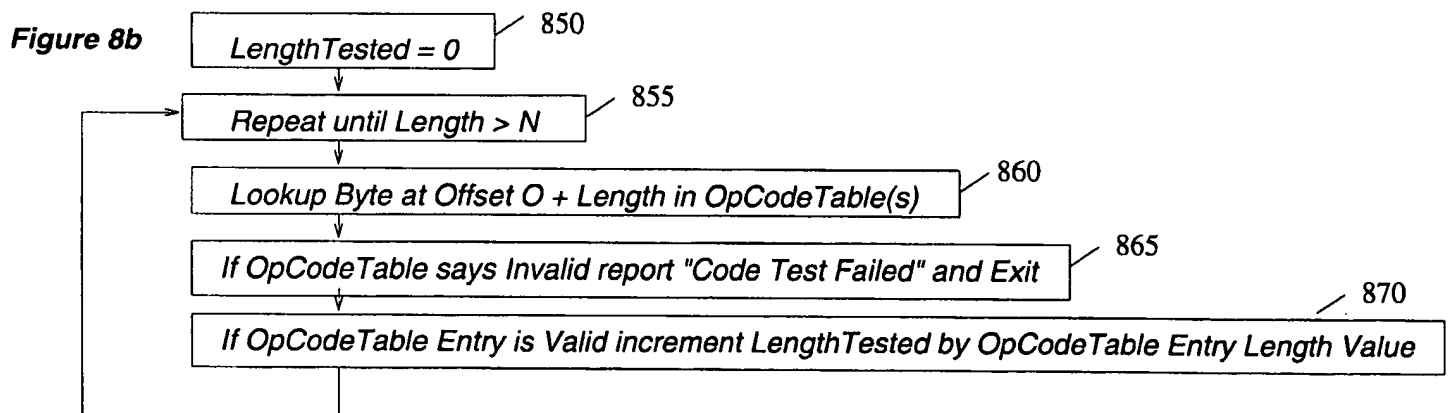
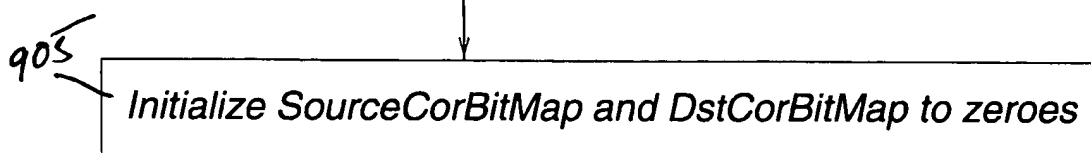
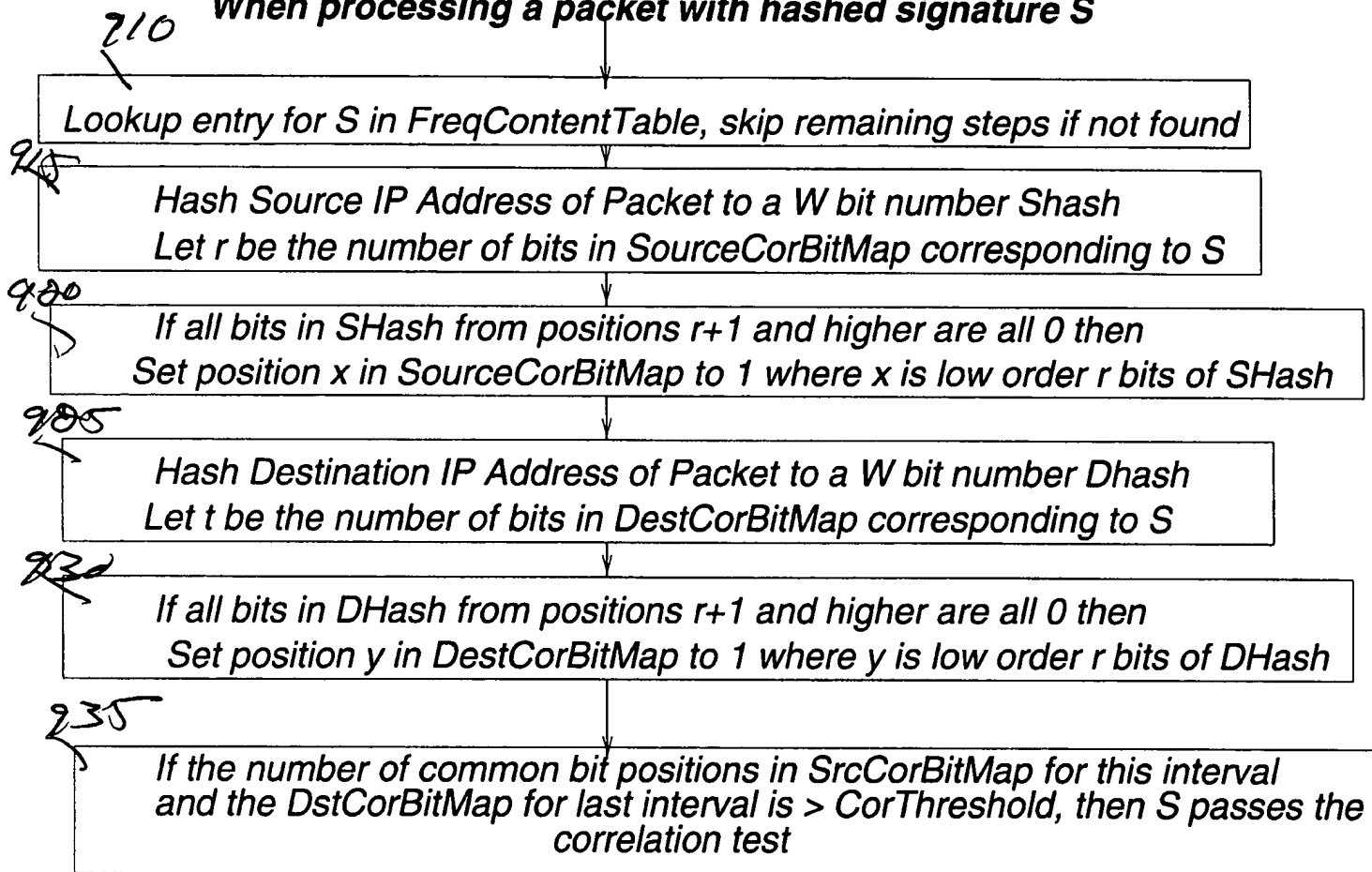


Figure 8: Code test as part of further tests (245) of the LSIDS system of Figure 2

When string S is added to FreqContentTable



When processing a packet with hashed signature S



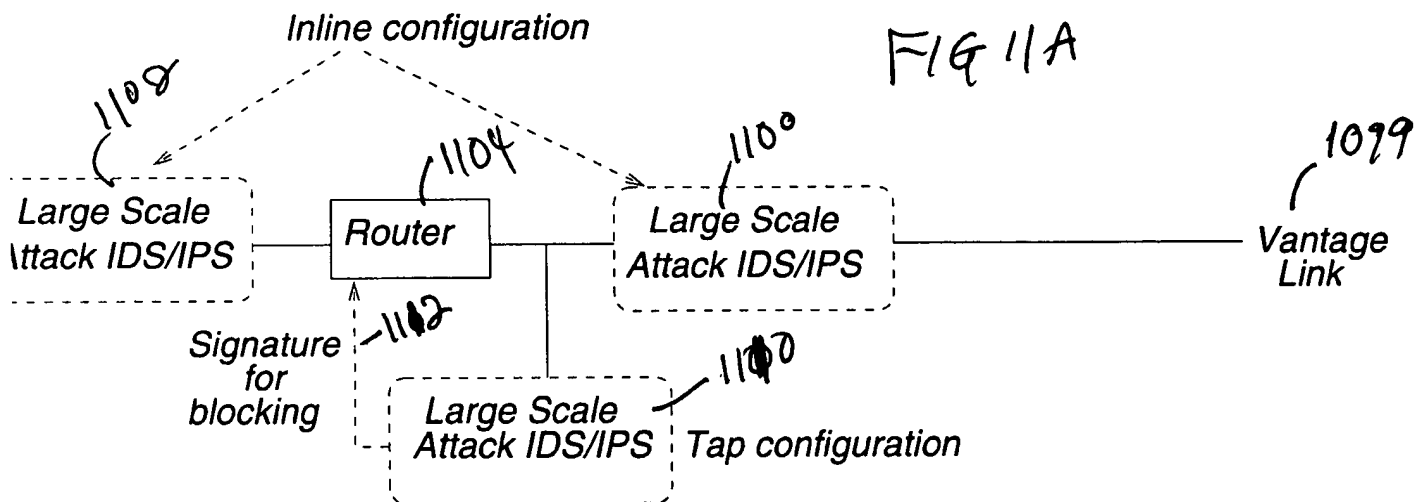
At end of interval for every suspicious signature S



Figure 9: Correlation test as part of the further tests (245) of the LISIDS system of Figure 2

If Signature S passes a Bayesian Spam test (an example is in Reference 3), then report that S passes the spam test

Figure 10: Spam test as part of the further tests (245) of the LSIDS system of Figure 2



Sample Intrusion Detection (IDS) and Prevention (IPS) Configurations

